Final

451-FPP-NCCDS-1998

NETWORK AND MISSION SERVICES PROJECT

Network Control Center (NCC) Data System(NCCDS) 1998

NCC Failover Plan and Procedures (FPP)

May 1999

National Aeronautics and
Space Administration

Goddard Space Flight Center
Greenbelt, Maryland

Final

Network Control Center Data System (NCCDS) 1998
NCC 98 Failover Plan and Procedures (FPP)

May 1999

Prepared Under Contract NAS 9-98100
Task: SODA NCC 98; Task Order G948
By
Computer Sciences Corporation

Prepared By:

R. Gaston Date
NCC 98 Initial Release Leader

Approved By:

J. Praytor Date
Technical Manager
NCC System Engineering

Quality Assured By:

M. Sanchez Date
NCC Quality Assurance Officer

Approved By:

D. DeSantis Date
Project Manager
NCC 98 SODA

Goddard Space Flight Center
Greenbelt, Maryland

Preface

Network Control Center Data System (NCCDS) 1998 (NCC 98) is the first step in migrating the NCCDS from the current proprietary system to an “open system” featuring a client/server architecture, substantial use of commercial off-the-shelf (COTS) products, and industry standard communications protocols.

Questions concerning this document or proposed changes shall be addressed to:

L. Myers
Code 451
Goddard Space Flight Center
Greenbelt, Maryland 20771

Abstract

This document summarizes the overall activities required to failover the operations of the Network Control Center Data System (NCCDS) Release NCC 98 from their primary facility to the alternate facility and back to their primary facility. While it covers failover for planned and catastrophic scenarios, this document is written from the perspective of planned failover from the primary facility to the alternate facility. It provides a general description of the activities necessary to change operational control from one equipment suite to the other.

Initially, the failover of NCC to an alternate facility and subsequent return requires extensive coordination between Operations personnel, System Administrators, and other support personnel. It is anticipated that this coordination can be reduced over time.

1 Introduction 1-1
1.1 Purpose 1-1
1.2 Scope 1-1
1.3 Document Overview 1-1
1.4 References 1-1
2 Failover Overview 2-1
2.1 General Description of Failover 2-1
2.2 Failover Scenarios 2-1
2.2.1 Planned Failover 2-1
2.2.2 Release Transition 2-2
2.2.3 Catastrophic Failure 2-2
2.3 Limitations 2-2
2.3.1 ANCC Limitations 2-2
2.3.2 Network Limitations 2-3
2.3.2.1 Assumptions 2-3
2.3.2.2 Procedures 2-3
2.3.3 Operating System Levels 2-3
3 Failover Activities 3-1
3.1 Failover Preparation 3-1
3.1.1 Cluster Preparation 3-1
3.1.1.1 RAID Contents 3-1
3.1.1.2 Internal Disks/Disk Farm 3-2
3.1.2 CCS VAX Preparation 3-2

3.1.2.1 Assumptions 3-3

3.1.2.2 Configuring the Operational System on the Development CCS/VAX 3-3

3.1.2.3 Transferring Back to the Operational CCS/VAX 3-4

3.1.2.4 Development Recovery 3-4

3.1.3 Workstation Preparation 3-5

3.1.4 Firewall Preparation 3-5

3.1.4.1 NCC 98 Baseline 3-6

3.1.4.2 Rules and Objects 3-6

3.1.4.3 Mproxy Configuration Files 3-6

3.1.5 NPG Preparation 3-6

3.1.5.1 NCC 98 Baseline 3-6

3.1.5.2 NPG System Configuration Files 3-7

3.1.6 SCD Preparation 3-7

3.1.6.1 SCD Configuration 3-7

3.1.7 WWW Server Preparation 3-7

3.1.7.1 NCC 98 Baseline 3-7

3.1.7.2 FTP Accounts 3-8

3.1.7.3 TUT Data 3-8

3.1.8 System Resources Infrastructure Segment (SRIS) Preparation 3-8

3.1.8.1 Internal DNS 3-8

3.1.8.2 External DNS 3-8

3.1.8.3 NTP Configuration 3-8

3.1.8.4 NFS Mount Points 3-9

3.1.9 SAS Preparation 3-9

3.1.9.1 Primary SPSR Cluster to ANCC SPSR Cluster Failover 3-9

3.1.9.2 Primary NPG System to ANCC System Failover 3-9

3.1.10 VLAN Manager 3-10

3.2 Failover to ANCC 3-10

3.3 Specialized Configurations 3-12

3.3.1 Configuring CCS1 and CCS2 to ANCC 3-12

3.3.1.1 CCS1 and CCS2 Preparation 3-12

3.3.1.2 Failover to CCS1 and CCS2 3-13

3.3.2 Configuration of ANCC Workstations with OCR Cluster 3-14

3.3.2.1 Workstation Preparation 3-14

3.3.3 Configuring SAS 2 with ANCC 3-14

3.3.3.1 Primary SPSR Cluster to ANCC SPSR Cluster Failover 3-15

3.3.3.2 Primary NPG System to ANCC System Failover 3-15

3.3.4 SAS1 to SAS2 Failover 3-16

ABBREVIATIONS AND ACRONYMS

1 Introduction

1.1 Purpose

The purpose of this Failover Plan and Procedures (FPP) document is to provide an overall script of activities necessary for the successful transfer of the Network Control Center Data System (NCCDS) function from the primary facility to the auxiliary facility. The auxiliary facility is designed as a temporary host in the event of catastrophic conditions that preclude the use of the primary facility.

1.2 Scope

The FPP encompasses the activities in preparation for and during a failover of the NCCDS from facility to facility in a planned and orderly manner. This document is written from the perspective of a planned failover of the NCCDS from its primary facility, the Operations Control Room (OCR) to the Auxiliary Network Control Center (ANCC). The general activities outlined in the plan and procedures are also applicable to moving from the ANCC to the OCR.

1.3 Document Overview

This document is divided into three sections. This section, Section 1, Introduction, provides a high-level scope and organization of the document. Section 2, Failover Overview, covers the general description of failover, the different failover scenarios and the auxiliary facility limitations. Section 3, Failover Activities, covers preparation for a failover and the procedures to follow during a failover.

1.4 References

The following documents are referenced by this document or contain related information.

- Network Control Center Data System (NCCDS) System Requirements, 1998, Revision 2 (Draft), April 1998, 530-SRD-NCCDS/1998.
- Interface Control Document Between The Network Control Center Data System and The Mission Operations Centers, May 1998, 530-ICD-NCCDS/MOC.
- Interface Control Document (ICD) between the Network Control Center (NCC)/ Flight Dynamics Facility (FDF) and the White Sands Complex (WSC), Revision 5, June 1997.
- Network Control Center (NCC) Communications and Control Segment (CCS) Computer Operators User’s Guide, January 1999, 451-USG-CCS-NCCDS98.

- NCCDS Protocol Gateway (NPG) Operator’s Guide Release 98.1, revision 5, January 1999, 451-NPGUG/NCC98.
- Firewall User’s Guide
- High Availability (HA) User’s Guide Release 98.1, Revision 1, January 1999
- Operations Engineer Handbook 532-HBNCC/OE
- NSM User’s Guide
- Cabletron SecureFast VLAN Manager User's Guide

2 Failover Overview

2.1 General Description of Failover

Because of its importance in space network (SN) operations, the NCC is classified as a national resource. This classification imposes requirements on the NCC to have an alternative location to perform operations. This requirement is in addition to the stringent reliability/maintainability/availability (RMA) requirements, which force the NCCDS to be designed to have full redundancy of configuration items (CIs) related to the fulfillment of the NCC's critical functions.

Two terms are used to describe how the NCCDS satisfies the above requirements: "*Switchover*" and "*Failover*." In general, "*Switchover*" describes how the NCCDS meets its RMA requirements (i.e., how control is transferred from a primary CI to its redundant CI in the event of a failure). "*Failover*" describes how the NCCDS meets its national resource requirements (i.e., how control is transferred from a primary location to its alternate location). This document focuses on the philosophy and procedures related to "Failover."

The primary location for NCC operations is the Operations Control Room (OCR) and its associated equipment rooms. These rooms located in Building 13 of the GSFC. The alternate location for NCC operations is the Auxiliary NCC (ANCC) and some associated equipment rooms. The ANCC is located in Building 3 of the GSFC with its associated equipment rooms being located in Building 13A. Thus, this document describes the failover of the NCCDS Operations from the OCR to the ANCC and vice versa.

2.2 Failover Scenarios

This document cannot capture all possible reasons or conditions that would cause NCCDS operations to be moved from one location to the other. Furthermore, every failover is unique in that certain steps may vary depending upon the initial status of either facility, the reason the failover was initiated, and the time requirements related to the failover.

However, the reasons that operations would failover from one location to the other can be generalized into three categories: planned failovers, transitioning from one NCCDS release to another, and unplanned failovers resulting from a catastrophic event or failure.

2.2.1 Planned Failover

Planned failovers are usually performed at regular intervals. The purpose of these planned failovers is to keep operations personnel familiar with the failover process, to exercise the equipment in the alternate location, and to satisfy contingency planning for support of Shuttle missions. Planned failovers are characterized by advanced notification, minimal time requirements, and careful review of procedures.

2.2.2 Release Transition

The transitioning from one NCCDS release to another usually requires a failover from one facility to the other. This failover is intended to make the equipment from one string available for modification to hardware and/or software. This allows new releases to be delivered to the operational environment with minimal interruption to ongoing operations. This type of failover is characterized by advanced notification, more stringent time requirements than a planned failover, and careful review or modification of procedures.

2.2.3 Catastrophic Failure

Failovers driven by a catastrophic failure or event, such as a fire, explosion, or power outage, are intended to restore NCC operations to the SN as quickly as possible. These failovers are characterized by no advanced notification, critical time requirements, and tailoring of procedures as necessary. Additional support personnel are usually on-hand to assist with time critical functions and to advise on the tailoring of procedures based on current needs and conditions.

Since it is impossible to address all potentially catastrophic failures or events, familiarization of the failover process through planned failovers is essential in restoring NCC operations as quickly as possible.

2.3 Limitations

While the ANCC is an alternate location for NCCDS operations, it is not equivalent to the OCR in terms of equipment. Specifically, the ANCC is not designed to satisfy the stringent RMA requirements levied against the NCCDS. For this reason, the ANCC is not intended to support NCC operations for extended periods (e.g., several weeks) of time.

2.3.1 ANCC Limitations

In its standard configuration, the ANCC has a single NPG, Firewall, Small Conversion Device (SCD), and Communication Control Segment (CCS) VAX. The lack of redundant nodes for these components limits the ANCC’s ability to meet all NCCDS RMA requirements. The lack of redundant nodes for these components also makes their configuration slightly different than its OCR counterpart.

In addition, the ANCC is limited to 6 workstations. This limits the number of positions (i.e., roles) that can be supported while operations is in the ANCC. Therefore, planned ANCC failovers should be avoided during heavy network testing periods and Shuttle support periods.

2.3.2 Network Limitations

2.3.2.1 Assumptions

The change of control from the OCR to the ANCC is facilitated by the network design of the NCC. Under the current configuration, the interior network does not have subnets. This lack of subnets allows the communications between the various components of the OCR and the ANCC to be controlled directly by the virtual local area network (VLAN) management configuration.

As mentioned previously, the ANCC's connectivity to Closed IONET is through a single Firewall. This architecture implies that Firewall failures require the primary (i.e., only) Firewall to be rebooted to restore communications to Closed IONET entities. Such reboots cause OSPF router updates to cascade through Nascom, potentially impacting data on that network. Therefore, the number of reboots should be minimized.

Outside of VLAN control, there exists an "automated workstation failover script" that allows certain personnel (TBD: end users or just System Administrators) to choose which suite of servers a workstation will connect to. This script can be executed from a captive account that will reconfigure the workstation and then reboot it.

2.3.2.2 Procedures

There are separate VLANs for Operations (OPS) and the ANCC. All systems on the interior network that communicate with the outside world via the firewalls will be assigned to the VLAN that is appropriate for their location. Systems that do not communicate through the firewalls can be assigned to either VLAN, or to both, which simplifies the mix-and-match process.

At this point in time, the following systems are anchored to a single VLAN:

- The cluster servers
- The NPGs
- The interior interfaces of the firewalls

All other interior network systems are eligible to be configured as floaters.

2.3.3 Operating System Levels

This document assumes that the operating system levels in the ANCC are the same as in the OCR. Failovers that take place during periods when the two facilities are at different operating system levels will require additional steps. These steps will be included in procedures developed for the specific equipment and operating systems on an as needed basis.

3 Failover Activities

3.1 Failover Preparation

3.1.1 Cluster Preparation

3.1.1.1 RAID Contents

The three items in the Redundant Array of Independent Disks (RAID) that must be addressed during failover are:

- Service Planning Segment Replacement (SPSR) Database
- "NFSHost"
- Automated Conflict Resolution System (ACRS)

Mirroring is employed to provide a current working copy of items for use in the ANCC or OCR. The procedures required to assure proper operation are documented in the Operations Engineer Handbook.

From ANCC Workstation	**From OCR Workstation**
Login to Restricted System Administration Manager (SAM) using special account	
Stop OET	
	Login to Restricted SAM using special account
	Select icon to Stop Ops
	Select icon to unmount local Network Files Services (NFS)
Select icon to mount remote NFS	
Mount the individual workstations	
Start Ops	

3.1.1.2 Internal Disks/Disk Farm

There are no changes required on the internal disks unless multiple versions of software exist that require the System Administrator to mount applicable versions.

If the OET Custom Applications baseline is at a different version than Operations then the disk farm disks will be physically swapped to the applicable version.

3.1.1.2.1 Oracle Binaries

This procedure only applicable if the version of Oracle in the OET baseline is different than the version in Operations.

The System Administrator will be required to move Oracle binaries from the internal disk drives to the disk farm or configure multiple copies of Oracle to support the applicable version.

3.1.1.2.2 ITO Application

This procedure only applicable if the version of the ITO application in the OET baseline is different than the version in Operations.

The System Administrator will be required to move ITO binaries from the internal disk drives to the disk farm or configure multiple copies of ITO to support the applicable version.

3.1.1.2.3 Omniback

This procedure only applicable if the version of the Omniback in the OET baseline is different than the version in Operations.

No changes are required for Omniback software when failing to the ANCC. However the Operations Engineer will be required to install the current tape magazine and manually execute a backup after failover.

3.1.1.2.4 Custom Applications

This procedure is only applicable if the version of the custom application in the OET baseline is different than the version in Operations.

In order to facilitate OET testing with different custom application versions, the Operations and OET disks will be swapped within the disk farm

3.1.2 CCS VAX Preparation

The Communications and Control Segment (CCS) failover procedures describe and document the steps required (1) to failover Network Control Center Data System (NCCDS) CCS operations from the CCS/VAX 1 and 2 (cluster) computer system to the CCS/VAX 3 computer system and (2) restore the development environment.

3.1.2.1 Assumptions

These failover procedures were developed based on several assumptions:

- For the operational CCS
  - During a CCS failover, an operational SPSR will be available.
  - During a CCS failover the CCS copy of the static data will be loaded from the static data failover tapes created during the last daily static data save of the operational CCS VAX. Subsequent updates will be retrieved from the operational SPSR during startup synchronization.
  - During a CCS failover or subsequent recovery, the CCS copy of the White Sands Complex (WSC) Schedule will be retrieved from the SPSR during startup synchronization
  - An operational disk on CCS3 will be available for a failover to the development CCS (CCS3).
- For the development CCS
  - A development disk will be available for recovery of the development environment on CCS3.

3.1.2.2 Configuring the Operational System on the Development CCS/VAX

This section presents the procedure to perform a failover from the operational CCS/VAX cluster (CCS1 and CCS2) to the development CCS/VAX computer (CCS3). This procedure includes a hardware device reconfiguration, and establishment of the operational CCS environment on the development CCS/VAX. The failover procedure consists of the following operator steps:

1. Shut down CCS software running on CCS3. The CCS computer operator does this through the system console described in the NCC CCS Computer Operator's manual.
2. Run the Release Selection Utility to select the correct operational release.
3. Static data tapes (SDTnnn) created between failover completion and CCS startup can be applied using the backup-static data restore procedures:

   Backup type: DAILY, WEEKLY, IMAGE, STATIC

   [D:DAILY]:

   a. Select the STATIC option.

      Perform Static Save or Restore?:

   b. Select the RESTORE option.

c. Mount the current failover static data tape on the device indicated by $1$MUA# (where # is the device number) in response to the following:

   ```
   >>>>MOUNT THE STATIC_DATA FAILOVER REEL
   (SDTnnn) <<<< %%%%%%%%%% OPCOM DAY-MONTH-YEAR HH:MM:SS
   %%%%%%%%%% Please mount volume SDTnnn in device
   $1$MUA#:(HSCDEV) %MOUNT-I-OPRST
   Please mount volume SDTnnn in device $1$MUA#:  (HSCDEV)
   ```

4. Start CCS software using the cold-start procedure described in the NCC CCS Computer Operator User’s Guide.

3.1.2.3 Transferring Back to the Operational CCS/VAX

The NCC continues to operate on the development CCS until the operational CCS/VAX cluster is made available for operational support. The technical manager (TM) decides when to transfer operations back to the operational CCS. This usually can be done between events with minimal impact on Operations. Note that the CCS/VAX operational baseline should still be intact or will have been restored at this point. A CCS cold start is performed, and operational support is resumed. The development CCS remains in operational mode until confidence in the operational CCS is restored.

3.1.2.4 Development Recovery

The development CCS is disconnected from the operational LAN. The development CCS software configuration is restored. The remote (from Building 13) development terminals are connected. The development CCS is patched to the remainder of the NCCDS development system. Finally, the operator performs a CCS cold start to verify the development restoration.

The CCS development recovery procedure is performed when CCS operations have been reestablished on the operational CCS following operational support on the development CCS. The development CCS hardware is reconfigured, and the software development environment is restored to resume development activities. This procedure reconfigures the development CCS/VAX hardware, and restores the software development environment. The operator takes the following steps:

1. Shut down CCS software. The CCS computer operator does this through the system console using the procedure described in the NCC CCS Computer Operator User’s Guide.

2. Shut down the VAX software. This is done by the CCS computer operator by using the system SHUTDOWN procedure described in the NCC CCS Computer Operator User’s Guide.

3. Spin down the operational disks by returning the RUN switches to a non depressed position.

4. Power off each operational drive by pressing the power switches located on the front of the storage array.

5. Power down HSC50. The operator performs this function by using the power switches inside the rear of the HSC cabinet. The power supply switch to the HSC terminal and printer must also be turned off.

6. Power up the HSC50 using the switches in the rear of the HSC.

7. Power on the development disks by pressing the power switches located on the front of the storage array.

8. Once the disk drives have completed their power up diagnostics, depress the RUN switches to spin up the drives.

9. 13. Boot the system using the standard bootup procedure described in the NCC CCS Computer Operators manual. Boot the VAX system (CCS3) using the standard bootup procedure described in the NCC CCS Computer Operator User's Guide.

10. Start CCS software using the cold-start procedure described in the NCC CCS Computer Operator User's Guide.

3.1.3 Workstation Preparation

If the version of the client application software in the OET baseline is different than the version in Operations, the System Administrator will perform steps to update or restore the proper version by softlink or other method.

3.1.4 Firewall Preparation

This procedure only applicable if the version of the firewall application software in the OET baseline is different than the version in Operations. Due to the special nature of the firewall application software (its tight coupling with the operating system), there will be two bootable disks in the ANCC firewall. One of the disks will be configured for OPS use, and the other will be available for testing alternate configurations in an OET environment. The software version of the firewall will be determined by which disk is used to boot the system. The software version (OPS or OET) can be changed by rebooting the firewall from the corresponding disk.

The ANCC firewall's OPS-Mode disk must be kept up to date with respect to any changes that are made to the OCR firewalls. This effort includes the operating system (and patches), the resident application software (firewall, mproxy, GateD, BIND, etc.), and the various applications' configuration files.

The OPS rule set and OPS mproxy configuration file must be loaded to ensure proper operation in OPS mode.

The OCR firewalls do not have the extra disks, and therefore will always be in OPS-Mode. Any changes made to the OCR firewalls for testing or troubleshooting should be undone at the conclusion of the test. The remainder of this section does not apply to the OCR firewalls.

3.1.4.1 NCC 98 Baseline

The NCC 98 Baseline can be restored on the ANCC firewall by booting from the OPS-Mode disk.

3.1.4.2 Rules and Objects

The firewall application's configuration files (rules and objects) can be restored by booting from the OPS-Mode disk.

3.1.4.3 Mproxy Configuration Files

If there are different versions of Firewall software for Operations and OET, then the mproxy configuration files will be restored by booting from the OPS-Mode disk. If Operations and OET are sharing a single disk drive, then the mproxy configuration file(s) can be restored to the Ops version by

- enter the file folder manager

access the applicable directory

- copy the operational mproxy files to the default folder (mproxy_config.mp)
- access the Mproxy GUI and terminate the Mproxy application (it should restart automatically).

This step must be performed after the correct Rules and Objects (Section 3.1.4.2) have been loaded.

3.1.5 NPG Preparation

The NPG system has three functional areas that must be changed to switch between OPS and OET modes. The file `/etc/ha_version` determines what level the high availability software will use. Each account on the NPG is tied to a particular version of the NPG and vector translator (VT) applications, so that switching versions is accomplished by logging into a different account and launching the applications. Finally, the configuration files for the NPG and VT applications are maintained within the server cluster, and are downloaded to the NPGs when so commanded by an operator.

3.1.5.1 NCC 98 Baseline

The file `/etc/ha_version` must be edited to reflect the desired mode ("ops", "oet", "it", etc.). Once this file has been changed, the system should be rebooted. The proper versions of the NPG and VT applications are selected by logging into an operator account that is tied to the desired version.

3.1.5.2 NPG System Configuration Files

The configuration files for the NPG and VT applications are maintained within the server cluster. The server can store multiple versions of the configuration files. An operator chooses the version to download to the NPG. This is accomplished by accessing the FTP option on the sub-panel under the NPG **xxxxxxx** icon on the toolbar. The software provides prompts that assist the operator in selecting the appropriate version.

3.1.6 SCD Preparation

Because the SCD software is developed and maintained by Nascom Integrated Services Network (NISN), this plan assumes that all SCDs would be upgraded at the same time. That is, the SCD software level will always be the same between operations and OET. If this assumption contradicted, special procedures will be developed for the specific software levels on an as needed basis.

3.1.6.1 SCD Configuration

The SCD configuration should be the same for operations and OET. However, when performing a failover, the SCD configuration should be reviewed for correctness. In particular, the serial interfaces should be reviewed to ensure that they are using the external clock for both reception and transmission of data.

After “unpatching” from the NTS, the SCD needs to be warm started to clear out any queued messages. After the warm start is complete, the operational interfaces from WSC can be patched, clock lines first.

3.1.7 WWW Server Preparation

If WWW Server application software in the OET baseline is different than the version in Operations, a portable tape drive is required to load the applicable software, since the WWW Server is isolated from the rest of the network.

3.1.7.1 NCC 98 Baseline

This procedure is only applicable if the version of the WWW Server application software in the OET baseline is different than the version in Operations.

The operational baseline must be restored during the failover. The baseline can be recovered by using the workstation restoration procedure with the Ignite-UX tape created for the WWW server.

The Ignite-UX workstation recovery process is documented in Appendix D of the Backup and Recovery Procedures document. The process requires an Ignite-UX tape of the machine to be restored and an account with *root* privileges.

NOTE

If sufficient disk space is available, the WWW server may be capable of having the operational and OET baselines resident on the disk at the same time. In this case, restoring the operational baseline may simply consist of the modification of several soft links to point to the correct software version.

3.1.7.2 FTP Accounts

"Operational" accounts should be identical on the OCR and ANCC TUTs. If additional test accounts have been added, the sysadmin should disable them (but not delete them). As a precaution, the sysadmin should also make sure that the file transfer directories ("incoming" and "xfer") are empty in each of the operational accounts.

3.1.7.3 TUT Data

When changing to an operational mode, the existing Tracking and Data Relay Satellite System (TDRSS) Unscheduled Time (TUT) data file should be removed. Once the operational SPSR server has been activated, a data transfer from the SPSR server to the TUT should be initiated.

Change the VLAN group for the Machintosh computer used for creating files for email of TUT

3.1.8 System Resources Infrastructure Segment (SRIS) Preparation

3.1.8.1 Internal DNS

The internal domain name server (DNS) does not need to be changed.

3.1.8.2 External DNS

The external DNS does not need to be changed. As described in the MOC ICD, the NCCDS host aliases are constructed by appending an "h" and a numeric digit to the NCCDS service name (e.g., schReqh1). The client should start with "h1" and increment by one if the requested connection is unsuccessful. The external DNS advertised by the NCCDS has every third address (i.e. the "h3", "h6", and "h9" aliases) resolving to the ANCC nodes providing the respective NCC service. This scheme relieves the MOC of the responsibility of knowing the current location of NCC operations.

Some MOCs, however, do not use DNS to resolve host addresses. Therefore, when Operations has moved to the ANCC, these customers must be explicitly informed to direct external communications to the ANCC addresses.

3.1.8.3 NTP Configuration

Most of the systems are configured as "broadcast clients", and will sync to whatever time is being broadcast within their VLAN. The cluster servers are responsible for broadcasting the time, and are configured to be clients of one of the VAXen. The cluster servers will need to be reconfigured to get their time from whichever CCS is assigned to their VLAN.

3.1.8.4 NFS Mount Points

NSF mount points will be managed with the Red disk / Black disk system or otherwise be changed manually by SysAdmin. No NFS changes are imposed solely by the failover of operations to the ANCC.

3.1.9 SAS Preparation

The following provides an overview of the procedures that must be followed in an NCC operational failover to the ANCC facility so that SAS continues to function after the failover. Both the SAS1 and SAS2 computer systems may support NCC operations from the ANCC. However, SAS1 is expected to provide primary support, as there is no reason to fail to SAS2 because of an NCC failover to ANCC. The procedures for failing between the SAS1 and SAS2 systems are described in Section 3.3.3. SAS supports the following variations of an operational failover to the ANCC:

Failover from the primary SPSR cluster to the ANCC SPSR cluster only
Failover from the primary NPG system to the ANCC NPG cluster only
Failover to or use of some of the ANCC workstations only
Any combination of the above

Operational use of ANCC workstations does not affect SAS so no further discussion of this option is required. The combination of the variations is a straightforward process so that too requires no further explanation. The remaining two variation are described separately below.

3.1.9.1 Primary SPSR Cluster to ANCC SPSR Cluster Failover

The following described the conditions and procedures that must be followed during an NCC failover from the primary SPSR cluster to the ANCC SPSR cluster to ensure SAS support during and after the transition.

1. Halt the SAS package on the primary SPSR cluster
2. Start the SAS package on the ANCC SPSR cluster

No manual configuration or commanding of the SAS server is required. Upon startup, the SAS package searches the network for a functioning SAS server and will automatically connect to the SAS server. The search order and preference of SAS servers is specified in the SAS HP-UX Component's configuration file on the SPSR cluster and is not expected to ever change. All SAS server functions (e.g., ground terminal data collection, interactive database access, report generation, etc.) remain fully functional during the transition and no data loss should occur.

3.1.9.2 Primary NPG System to ANCC System Failover

The following describe the conditions and procedures that must be followed during an NCC failover from the primary NPG system to the ANCC NPG system to ensure SAS support during and after the transition. The following assumes a VLAN configuration in which the VLAN to which the SAS server is a member only contains the operational NPG or the ANCC NPG (not both) at any instant in time.

An NCC operations failover to the ANCC facility requires no manual configuration or commanding of the SAS server but does require that certain procedures are followed with respect to the NPG and VLAN changes. For the SAS server to detect a failover to the ANCC and automatically reconfigure itself for support the ANCC configuration, the following must be performed:

1. Shutdown the primary NPG system in an orderly manner so that SAS detects the loss of communication with the NPG
2. Change the SAS server's VLAN membership to that of the VLAN containing the ANCC NPG
3. Start the ANCC NPG system

If these procedures are followed, the SAS server will automatically search for and connect to the ANCC NPG following the loss of communications with the primary operational NPG system. The search order and preference for NPG systems is specified in the ground terminal client configuration file on the SAS server and is not expected to ever change. Except for the receiving of status from the ground terminals (ODMs, OPMs, and SLRs), all other SAS functions remain fully functional during this transition. The SAS DBA must manually edit the SAS database to correct for the loss of data from the ground terminal for the period of time during the transition from the primary NPG to the ANCC NPG.

3.1.10 VLAN Manager

The VLAN management software has been installed in two locations: on the dedicated Switch Management workstation (in room 141), and on the ANCC NPG. The Cabletron switches can be managed from either location, but only one of the instances can be active at any point in time. If it is necessary to transfer control from one switch management location to the other, the VLAN Manager and the VLAN Server applications must first be halted on the original system before being started on the other.

The VLAN management software keeps a database of the network and switch configurations. This database must be kept current on both switch management locations (Rm. 141 and ANCC).

3.2 Failover to ANCC

Once the preparation for the failover has been completed, control of NCC operations must be transferred from the OCR suite to the ANCC suite. This change of control requires the following steps to be performed:

- from the VLAN management station, put ANCC internal Firewall interface in “jail.”
- shutdown the OET Shadow Tool!
- shutdown the OET packages running in the ANCC, if necessary. This step can be performed as far in advance as necessary.

Logging into a failover account on a*sv0* and executing the desired Restricted SAM script (Stop OET) performs this step. This script can be executed by double-clicking on the appropriate icon (or through command line entry)

- shutdown the OPS packages running in the OCR. This step should not be performed until the desired failover time arrives.
- Logging into a failover account on *sv0* and executing the desired Restricted SAM script (Stop OPS) performs this step. This script can be executed by double-clicking on the appropriate icon (or through command line entry)
- Stop the NPG processes on the primary NPG system. This step ensures that the SAS server recognizes an NPG transition and automatically begins attempting to connect to the ANCC NPG. This step must be performed prior to changing the SAS server's VLAN membership to the ANCC network.
- Start the OPS packages to run in the ANCC. This step can be performed immediately after the previous shutdown step has completed.
- Logging into a failover account on *asv0* and executing the desired Restricted SAM script (Start OPS) performs this step. This script can be executed by double-clicking on the appropriate icon (or through command line entry)
- "unpatch" and warm start the SCD (to clear out any queued messages). After the warm start is complete, the point-to-point operational interfaces can be patched, clock lines first.
- cold start CCS. This step can be performed once the a*sn_oracle* and *accshost* packages are running. The procedure for this step can be found in Section 2.2.1 of the Network Control Center (NCC) Communications and Control Segment (CCS) Computer Operators User's Guide, January 1999.
- start the NPG processes. This step can be performed once *asn_oracle* and *aspsrhost* packages are running. At this point, the ground terminal communications should be restored and the reception of ODMs should begin. The procedure for this step can be found in Section 3 of the NCCDS Protocol Gateway (NPG) Operator's Guide Release 98.1, January 1999.
- move the internal ANCC Firewall interface out of "jail" and into the ANCC V-LAN group. This change completes the change of control and should be performed only after the above steps have been successfully completed. The procedure for this step can be found in the Cabletron SecureFast VLAN Manager User's Guide

NOTE

"Change of control" also includes steps related to voice communications, electronic mail, and other logistical changes that are outside the scope of this document.

3.3 Specialized Configurations

Because of limitations of the ANCC, limited time constraints, equipment availability, and other unforeseen circumstances, it is desirable to be able to support operations with various combinations of OCR and ANCC equipment. Two specific specialized configurations have been identified as being particularly useful to operations. These two configurations are described in the following sections.

3.3.1 Configuring CCS1 and CCS2 to ANCC

As stated previously, the nominal ANCC configuration consists of a single CCS VAX processor (CCS3). In the event that Operations must be supported from the ANCC for an extended period of time, eliminating this single point of failure would be very beneficial.

3.3.1.1 CCS1 and CCS2 Preparation

As stated previously, the nominal ANCC configuration consists of a single CCS VAX processor (CCS3). In the event that Operations must be supported from the ANCC for an extended period of time, eliminating this single point of failure would be very beneficial.

In order to configure CCS1 and CCS2 with the ANCC the following changes must be enacted.

- CCS1 and CCS2 must be moved into the ANCC V-LAN from the LAN Manager console The procedure for this step can be found in the Network Control Center (NCC) Communications and Control Segment (CCS) Computer Operators User's Guide, January 1999. This step can be performed any time CCS1 and CCS2 are not supporting Operations or OET.

- CCS1 and CCS2 must have its DNS tables deleted and its DNS (source) location changed to the appropriate server (e.g., anfshost). Currently, the System Administrator is required to execute this procedure. Specifically, files must be deleted and the command "**multinet ….DOMAINNAMESERVER reload**" must be run. This step can be performed once CCS1 and CCS2 are moved to the appropriate V-LAN group. This step should be confirmed by the command "nslookup npgz" returning the expected IP address.

- The ObjectBroker configuration on CCS1 and CCS2 must be modified to recognize the new cluster packages. Specifically, the command **@LOAD_CTX localhostnnnnnnn.col** must be executed, where "nnnnnnn" is the correct choice of *accshost* (ANCC) or *ccshost* (OCR). This step can be performed any time CCS1 and CCS2 are not supporting Operations or OET. This step can be confirmed by the command "appl/bro show context/system".

- modify the location of the CCS Log File Archive mount point to *anfshost*. This change requires System Administration support and modifies the **SYS$MGR:[]VMS_SYSSTARTUP** file.
- The applicable ccshost package (*accshost* or *ccshost*) is running on one of the nodes of the 3-node cluster. The ObjectBroker configuration of one of the other servers can be changed in preparation for the failover to CCS 1 and CCS2. This change can be enacted through the command "**./loadsysctx nnnnnnnccs12.col**", where "nnnnnnn" is the correct choice of *accshost* (ANCC) or *ccshost* (OCR). This command should be run from the */spsr/ccs/OBB* directory on the desired machine and requires *spsd/users* privileges. This step should not be performed until immediately prior to the failover, as it will cause problems if the ccshost in question unexpectedly switches to that node because of a failure. This step can be verified by entering the command **obbshctx –S** after completing the previous command.

At this point, the system is ready for the identification of a "least impacting" window for the failover.

3.3.1.2 Failover to CCS1 and CCS2

Once the preparation of CCS1 and CCS2 has been completed, control of real-time services must be transferred from CCS3 to CCS1 and CCS2. This change of control requires the following steps to be performed:

- halt STARTCCS on CCS3. The procedure for this step can be found in the Network Control Center (NCC) Communications and Control Segment (CCS) Computer Operators User's Guide, January 1999.
- move *accshost* from its current node to the node with the modified ObjectBroker system context. The procedure for this step requires the OE to access Restricted SAM and drill down to the "Package Configuration" icon. Through this icon, the OE selects the ccs_service package and chooses **Move Package** from the **Actions** menu.
- FTP the correct NPG configuration files (or modify the existing one) to the NPG and restart the NPG application. The correct NPG configuration has an entry for *ccsone* and *ccstwo*. port 3000, in the *endpoint.npg* file. Restarting the NPG application can be accomplished by selecting **Shutdown NPG** from **File** menu. The high availability (HA) software will restart the NPG application automatically with the correct configuration.

- modify the ObjectBroker system context on all applicable servers and workstations (through the **./loadsysctx** command described above).
- start STARTCCS on CCS1 or CCS2. The procedure for this step can be found in the Network Control Center (NCC) Communications and Control Segment (CCS) Computer Operators User's Guide, January 1999.
- at some point after the CCS failover, the NTP configuration for the ANCC servers must be modified to receive time from CCS1 and CCS2. This change is not time critical. This change must be performed by a System Administrator.

3.3.2 Configuration of ANCC Workstations with OCR Cluster

3.3.2.1 Workstation Preparation

Utilize the "automated workstation failover script" to configure the workstation for use with the OCR cluster.

3.3.3 Configuring SAS 2 with ANCC

Attached is a description of the procedures required for SAS to support a failover to the ANCC. No special procedures are required to be performed on the SAS server itself. The attached procedures generally have to do with what has to be done with the NPG and SPSR servers so SAS will transition correctly.

The following provides an overview of the procedures that must be followed in an NCC operational failover to the ANCC facility so that SAS continues to function after the failover. Both the SAS1 and SAS2 computer systems may support NCC operations from the ANCC. However, SAS1 is expected to provide primary support, as there is no reason to fail to SAS2 because of an NCC failover to ANCC. SAS supports the following variations of an operational failover to the ANCC:

1. Failover from the primary SPSR cluster to the ANCC SPSR cluster only
2. Failover from the primary NPG system to the ANCC NPG cluster only
3. Failover to or use of some of the ANCC workstations only
4. Any combination of the above

Variation 3, operational use of ANCC workstations does not affect SAS so no further discussion of this option is required. Variation 4, the combination of the variations is a straightforward process so that too requires no further explanation. The remaining two variation are described separately below.

3.3.3.1 Primary SPSR Cluster to ANCC SPSR Cluster Failover

The following describes the conditions and procedures that must be followed during an NCC failover from the primary SPSR cluster to the ANCC SPSR cluster to ensure SAS support during and after the transition.

1. Halt the SAS package on the primary SPSR cluster
2. Start the SAS package on the ANCC SPSR cluster

No manual configuration or commanding of the SAS server is required. Upon startup, the SAS package searches the network for a functioning SAS server and will automatically connect to the SAS server. The search order and preference of SAS servers is specified in the SAS HP-UX Component's configuration file on the SPSR cluster and is not expected to ever change. All SAS server functions (e.g., ground terminal data collection, interactive database access, report generation, etc.) remain fully functional during the transition and no data loss should occur.

3.3.3.2 Primary NPG System to ANCC System Failover

The following describe the conditions and procedures that must be followed during an NCC failover from the primary NPG system to the ANCC NPG system to ensure SAS support during and after the transition. The following assumes a VLAN configuration in which the VLAN to which the SAS server is a member only contains the operational NPG or the ANCC NPG (not both) at any instant in time.

An NCC operations failover to the ANCC facility requires no manual configuration or commanding of the SAS server but does require that certain procedures be followed with respect to the NPG and VLAN changes. For the SAS server to detect a failover to the ANCC and automatically reconfigure itself for support the ANCC configuration, the following must be performed:

1. Shutdown the primary NPG system in an orderly manner so that SAS detects the loss of communication with the NPG
2. Change the SAS server's VLAN membership to that of the VLAN containing the ANCC NPG
3. Start the ANCC NPG system

If these procedures are followed, the SAS server will automatically search for and connect to the ANCC NPG following the loss of communications with the primary operational NPG system. The search order and preference for NPG systems is specified in the ground terminal client configuration file on the SAS server and is not expected to ever change. Except for the receiving of status from the ground terminals (ODMs, OPMs, and SLRs), all other SAS functions remain fully functional during this transition. The SAS database administrator, (DBA) must manually edit the SAS database to correct for the loss of data from the ground terminal for the period of time during the transition from the primary NPG to the ANCC NPG.

3.3.4 SAS1 to SAS2 Failover

This section describes the use of the SAS2 computer to support the ANCC facility. The ANCC is normally supported by the SAS1 computer but the SAS2 computer is capable of supporting both the normal operational equipment suite and the ANCC equipment suite. While the SAS2 computer is capable of supporting the most important operational functions, it is only expected to be used for operational support during exceptional circumstances when the SAS1 system is inoperable for an extended period of time. The procedure to fail to the SAS2 computer with either the primary operational suite of equipment or the ANCC equipment is the same. When the SAS2 computer starts up, it will connection to which ever equipment suite it finds on the network it is connected to. The following is merely an overview of the failover process. More detailed procedures are contained in NCC LOP 024. Both the following description and LOP 024 describe a routine failover in which the basic integrity of the operational system was intact at the time of the failover. Refer to the applicable version of the SAS Operations Manual for recovery procedures if the integrity of the operational system was significantly compromised (e.g., there was significant file system damage) at the time of the failover.

Transferring responsibility of operational support from the SAS1 to SAS2 system involves the following steps:

1. Halt the SAS package on the OCR SPSR cluster
2. Shutdown all software on both SAS1 and SAS2 systems
3. Remove and store the disks from the SAS2 system
4. Remove the disks from the SAS1 system and install them in the SAS2 system
5. Reconfigure the NACC and Cabletron switches to disconnect the SAS2 system from the development network and connect it to the operational ANCC network
6. Initiate an auto-boot of the SAS2 computer
7. Start the SAS package on the ANCC SPSR cluster

The failover process is designed to be largely automatic and not to involve any manual reconfiguration beyond that of the network reconfigurations. Although there are slight differences between the two SAS systems (e.g., different peripherals, different number of NICs, different IP addresses, etc.), the auto-boot procedure will automatically take these into account. The SAS2 computer will also auto-boot the current operational revision of all commercial and application software even if the computer had been running different revisions of the software before the failover. Also note that the network identity (name and address) of the SAS2 computer will automatically be that of the operational SAS2 computer and not that of the operational SAS1 computer or that of the development SAS2 computer.

Once all the commercial and applications software has started up on the SAS server and the SAS package on the SPSR server is started, the SAS package automatically finds and establishes connections to the SAS2 computer. The SAS package will then proceed to update the SAS database with any changes to the SN schedule that occurred during the failover process. Similarly, upon startup, the Data Acquisition Component (DAC) software residing on the SAS server will establish connections to the NPG and begin buffering real-time information from the ground terminals. The DAC software on the SAS server will also evaluate the state of the SAS database and then prompt the operator for the CCS log tapes required to recover the real-time data that was missed during the failover process. Once the missing data has been recovered from tape, the data buffered during the tape processing period will be debuffered. Debuffering is performed at a faster rate than new data is received so the system will eventually transition to processing the information from the ground terminal in real-time. The message buffering transitions are all performed automatically by the software and the only operator support required is to supply the CCS log tapes.

Abbreviations and Acronyms

ACRS	Automated Conflict Resolution System
ANCC	Auxiliary Network Control Center
CCS	Communications and Control Segment
CI	Configuration Item
CM	configuration management
COTS	commercial off-the-shelf
DBA	database administrator
DNS	domain name server
FPP	failover plans and procedures
FTP	file transfer protocol
GSA	general service agreement
GSFC	Goddard Space Flight Center
HA	high availability
HP	Hewlett-Packard
ICD	interface control document
IP	internet protocol
LAN	local area network
MOC	Mission Operations Center
NACC	network access control card
NASA	National Aeronautics and Space Administration
Nascom	NASA communications
NCC	Network Control Center
NCCDS	Network Control Center Data System
NCD	NCC Central Delogger
NFS	network file service

NISN	NASA Integrated Services Network
NPG	NCC Protocol Gateway
NTP	network time protocol
OCR	Operations Control Room
ODM	Operations Data Message
OET	Operational Evaluation Testing
OPM	Operations Message
OPS	Operations
OSPF	Open shortest path first (TCP/IP routing protocol)
RAID	Redundant Array of Independent Disks
RMA	reliability/maintainability/availability
SAS	service accounting segment
SAM	System Administration Manager
SCD	small conversion device
SLR	Service Level Report
SN	space network
SODA	Space Operations Directive Agreement
SPSR	service planning segment replacement
SRIS	system resources infrastructure segment
STGT	Second TDRSS Ground Terminal
TDRSS	Tracking and Data Relay Satellite System
TM	Technical Manager
TUT	TDRSS unscheduled time
VAX	virtual address extension
VLAN	virtual LAN
VT	vector translator
WSC	White Sands Complex
WSGT	White Sands Ground Terminal

WWW	World-Wide Web